Wie funktioniert die Blockchain?

von Leonie Frink

Leonie hat Rechts- und Wirtschaftswissenschaften studiert und beginnt demnächst ihr Referendariat. Sie interessiert sich gerade besonders für die Blockchain-Technologie.

Die Person hinter dem Namen Satoshi Nakamoto umgeben viele Geheimnisse. Dennoch ist sicher, dass sie 2008 den Genesis-Block der Bitcoin-Blockchain erzeugte. Die Finanzinstitute hatten zu dieser Zeit infolge der Finanzkrise das Vertrauen vieler Anleger verspielt und so war Nakamotos Blockchain-Technologie, die sichere monetäre Transaktionen ohne vermittelnde Bank realisieren konnte, revolutionär.

Aus der Geschichte der Blockchain erklären sich ihre typischen Charakteristika: Das Blockchain-System ermöglicht eine direkte Kommunikation der Teilnehmer (peer-to-peer) und bietet trotz deren Anonymität eine besonders hohe Gewähr für die Wahrheit der gespeicherten Informationen.

Doch wie funktioniert die Blockchain-Technologie?

Die Blockchain besteht aus miteinander verketteten Blöcken. Ein Block enthält bestimmte Informationen, die jeglicher Art sein können. Im Fall von Bitcoin können in einem Block beispielsweise verschiedene Transaktionen gebündelt werden. Sollen nun Informationen dieses Blocks verändert werden, wird dieser nicht etwa gelöscht oder umgeschrieben, stattdessen werden die Informationen in einem neuen Block gespeichert und mit dem alten Block verkettet. Die Blockchain kann dadurch niemals rückwirkend verändert werden und die Interaktionen im System bleiben stets sichtbar.
Dabei heißt sichtbar nicht zwangsläufig bekannt. Die im Block enthaltenen Informationen, beispielsweise die Identität des agierenden Teilnehmers, können selbst kryptografisch verschlüsselt sein. Die Blockchain wird typischerweise mit einem asymmetrischen Kryptosystem kombiniert. Anders als bei symmetrischen Kryptosystemen, bei welchen alle Teilnehmer denselben Code zur Ver- und Entschlüsselung nutzen, erhält bei asymmetrischen Kryptosystemen jeder Teilnehmer einen eigenen Public und einen Private Key. Der Public Key verschlüsselt die Nachricht und dient dazu, dass sie nur von demjenigen gelesen werden kann, für den sie bestimmt ist. Mit dem Private Key kann der Empfänger die Nachricht entschlüsseln. Mit ihm werden die im Blockchain-Netzwerk geteilten Informationen digital signiert. So kann ein Identitätsnachweis erbracht werden, ohne die Identität selbst preisgeben zu müssen und die Teilnehmer können komplett anonym agieren.

Die Verwaltung der Blockchain erfolgt dezentral. Das führt dazu, dass Fälschungen oder abgeänderte Kopien ausgeschlossen sind. Die Teilnehmer eines Netzwerks interagieren über die sogenannten Nodes (Knotenpunkte). Die Interaktion erfolgt somit direkt zwischen den Teilnehmern (peer-to-peer), ohne einen Mittelsmann. Wird eine neue Transaktion vorgenommen, wird diese im Hintergrund an alle Nodes des betroffenen Netzwerks zur Überprüfung versendet. Durch die Nutzung des Public Key ist die Integrität dieser Nachrichten gesichert. Die Nodes senden die Transaktion wiederum an alle ihnen bekannten Nodes weiter, bis die Transaktion schließlich allen Nodes des Netzwerks bekannt ist. Neue Nodes im System müssen dabei die gesamte Blockchain kopieren.

Die Verkettung der Blockinformationen erfolgt durch den sogenannten Hash-Wert. Durch Hash-Werte wird die Integrität von Daten gesichert. Der Hash ist eine mathematische Rechenformel, bei der ein Input immer, aber zwei verschiedene Inputs niemals denselben Wert ergeben. Die Nutzer des Netzwerkes können durch den verknüpfenden Hash-Wert auf die Wahrheit der Daten-Historie vertrauen. Sollte jemand die Daten eines Blocks verändern, ändert sich auch der Hash-Wert dieses Blocks, sodass dieser nicht mehr zu dem nachfolgenden Block passt. Die Blockchain bricht dann an dieser Stelle.

Um vor Missbrauch zu schützen wird ein neuer Block erst dann als valide anerkannt und mit der bisherigen Blockchain verkettet, wenn die Hash-Werte durch eine gewisse Anzahl sogenannter Miner überprüft wurden. Die Miner sorgen dafür, dass das Netzwerk auf die Wahrheit der in der Blockchain enthaltenen Informationen vertrauen kann und ein Konsens über die aktuelle Datenlage besteht. Da die Blockchain nicht rückwirkend verändert werden kann, besteht der Konsens des Netzwerks immer über die längste existierende Blockchain. Die Miner überprüfen durch kryptografisch-mathematische Berechnungen die Hash-Werte. Die Validierungsalgorithmen garantieren die Vertrauenswürdigkeit der in der Blockchain aufgezeichneten Daten. Hierdurch wird es überflüssig, die Information durch einen vertrauenswürdigen Dritten (bspw. Banken, Notare oder Treuhänder) verifizieren zu lassen.

Für diese Überprüfung ist eine gewisse Rechenleistung erforderlich, die die Miner bewältigen. Die Betreiber des Lefdal Mine Datacenter haben das Mining bereits professionalisiert. In einer ehemaligen Mineralmine in Norwegen werden in riesigen Containern Hochleistungsrechner betrieben, die rund um die Uhr neue Blöcke validieren. Das kühle Umfeld ist perfekt, die Rechner können mit dem Wasser aus dem nahegelegenen Fjord gekühlt und der benötigte Strom aus Wasserkraft gewonnen werden.
Die meisten Blockchain-Netzwerke nutzen diese sogenannte Proof-of-Work-Methode um Konsens im Netzwerk zu schaffen. Hierbei erhält derjenige Miner, der den Block als erstes validiert, den Zuschlag für die Erstellung des Blocks und eine Belohnung für seine Leistung. Daneben gibt es noch die Proof-of-Stake-Methode, bei

der zwar mehrere, aber ausgewählte Prüfer die Blockinformationen validieren, und die Proof-of-Authority-Methode, bei der der Validierungsprozess bei einer Autorität zentralisiert ist.

Bis heute steht der Bitcoin im Volksmund stellvertretend für die Blockchain. Die Nutzung für monetäre Transaktionen ist aber nur eine naheliegende Anwendung der Blockchain. Die Blockchain kann jegliche Informationen transportieren. Derzeit gehört die Blockchain-Technologie aufgrund ihres großen Potentials für neue Anwendungen zu den vielversprechendsten Technologien der Zukunft. Da das Blockchain-System niemanden ausschließt, ermöglicht es einem großen Teil der Weltbevölkerung erstmals überhaupt schrankenfrei am internationalen Austausch und Handel teilzunehmen. Viele Unternehmen eruieren ihre Möglichkeiten zur Nutzung der Blockchain und verwenden für interne Anwendungen immer häufiger dezentralisierte Systeme, durch die unter anderem Störungen besser abgefedert werden können. Darüber hinaus wird die Blockchain vor allem in Verbindung mit Smart Contracts und dem Internet of Things diskutiert. Insbesondere die hohe erforderliche Rechenleistung bei der Validierung der Daten, die zu einem gleichsam hohen Stromverbrauch führt und die auf der Blockchain laufende Anwendung deutlich verlangsamt, steht allerdings in der Kritik. Zudem sind noch nicht alle Probleme hinsichtlich Skalierbarkeit und Interoperabilität gelöst.

Weiterführend:

Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008, https://bitcoin.org/bitcoin.pdf (zuletzt abgerufen am 10.01.2021)

Schlatt/Schweizer/Urbach/Fridgen, Blockchain: Grundlagen, Anwendungen, Potentiale, White Paper des Fraunhofer-Instituts, 2016, https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf (zuletzt abgerufen am 10.01.2021)

Blockchain-Labor des Fraunhofer-Instituts, Experience Lab für Technologien, Implementierungen und Anwendungen, https://www.fit.fraunhofer.de/de/fb/cscw/blockchain.html (zuletzt abgerufen am 10.01.2021)

Die Blockchain-Revolution, Dokumentation vom 24.01.2019 in der 3Sat-Mediathek, https://www.3sat.de/wissen/wissenschaftsdoku/die-blockchain-revolution-104.html (zuletzt abgerufen am 10.01.2021)

SAP Insights, Was ist eine Blockchain?, https://www.sap.com/germany/insights/what-is-blockchain.html (zuletzt abgerufen am 10.01.2021)

Zu Kryptowährungen und Blockchain https://blockchainwelt.de (zuletzt abgerufen am 10.01.2021)

Talking Legal Tech - Folge 5:
„was ist die blockchain,
florian glatz?“